Radiation Detection Information Barriers

James L. Fuller
Pacific Northwest National Laboratory

Presentation Topics

- Background
- What is an “Information Barrier” (IB)?
- IB Functional Requirements
- Basic Design Criteria for Information Barriers
- Authentication of Measurement Systems

Background

- The U.S. has been studying information barriers in a coordinated manner, for possible use in the monitoring of classified nuclear materials, since January 1999.
- We have reached some initial conclusions through an inter-laboratory and inter-agency process.
- We briefed some of these conclusions to Russian counterparts during the LLNL TEG meeting in April 1999 and during the Trilateral Initiative demonstration at Los Alamos in June 1999.
- A more detailed briefing was presented in Moscow in December 1999 to Russian Federation representatives.

What Is an "Information Barrier"?

- **A radiation detection system information barrier consists of procedures and technology that prevent the release of sensitive nuclear information during measurement of a sensitive item, and it provides confidence that the measurement system functions as designed and constructed.**

IB Functional Requirements

- **The host must be assured that host classified information is protected from disclosure to the monitoring party.**

- **The monitor must be confident that the integrated system measures, processes, and presents the conclusion in an accurate and reproducible manner.**

The requirement to protect host country classified information is paramount.

Basic Design Criteria for Information Barriers

Basic Design Elements

- Equipment Certification
- Central Processing Unit (CPU)
- Non-CPU Equipment
- Procedural Issues
- Electronic Emanation Considerations
- Multiple/Intermediate Barriers
- Software, Firmware, and CPU Operating Systems
- Inputs and Outputs
- Measurement System Authentication and Repair

Equipment Certification

Issue: **Assure that hardware will not reveal classified information.**

Solution: **Host country "certifies" equipment as meeting its own security requirements.**

Central Processing Unit (CPU)

Issue: **All digital processing must be trusted and inspectable.**

Solution: **Use "trusted" processors (processors that are dedicated to specific tasks and have extraneous functionality eliminated, such as single-board computers).**

Non-CPU Equipment

Issue: **All non-CPU functions must be trusted and inspectable.**

Solution: **HPGe systems and related subsystems are probably inherently inspectable. Other radiation detection subsystems must be considered on a case-by-case basis.**

Procedural Issues

Issue: **Avoid deduction of classified information simply by observation of system setup.**

Solution: **Case-by-case evaluation required, but in general instrument must be able to accommodate all anticipated variations in measurement conditions without revealing classified information.**

Electronic Emanation Considerations—Host

Issue: **Host must be assured that no electronic emanations from measuring system can be recorded by monitoring party.**

Solution: **Equipment should be evaluated for emanations according to standards and practices acceptable to host.**

Electronic Emanation Considerations—Monitor

Issue: **Monitoring party must be assured that host cannot dupe them by electronic means.**

Solution: **The monitoring party will have to perform system-level assessment of risk and might demand rigorous emanation protection even under trusted-processor arrangements.**

Multiple/Intermediate Barriers

Issue: **Enhancement of security through the use of several information barriers that are "layered."**

Solution: **If intermediate barriers can be employed without compromising functionality assurances, then it may be desirable to do so.**

Software, Firmware, and CPU Operating Systems

Issue: **Computer code inspectability.**

Solutions: **Software at every level must be completely inspectable and documented.**

The amount of code must be minimized.

Complex operating systems and compilers must be avoided.

Inputs and Outputs

Issue: **I/O required, but complicates inspectability.**

Solution: **All I/O must have a well-understood, dedicated function, with no extraneous ports/devices associated with the measurement system; simple displays should be used for yes/no type output results, peripherals must be minimized, and bus structures avoided.**

Measurement System Authentication and Repair

Issue: **Monitoring integrity of equipment during system authentication and repair activities.**

Solution: **Multiple copies of host-provided equipment should be maintained under secure storage, with the monitoring party selecting one for examination upon demand.**

Software should be similarly supplied on demand, particularly before first use.

Most defective equipment should be discarded and replaced (detector heads excepted).

Design Basis Summary

- Both sides must have their own assurance that information barriers completely protect classified information while providing adequate confidence that the measurement system is operating properly.

- The U.S. assessment is that there are a limited number of basic design criteria that need to be considered, that there are procedural and technological solutions available, but that in the end, each system must be assessed on a case-by-case basis.

- The U.S. assessment of the problem is that cooperative development of information barriers provides for the greatest degree of trust and transparency.

Demonstration System IB Summary

- Equipment certification: host (U.S.) supplies/certifies the system as meeting its own security requirements and controls access to and retains the system.
- CPUs: N+1 single-board processors are used (a possible next cooperative step could be to reduce number of CPUs used).
- Non-CPU equipment: some documented commercial equipment is used (a possible next cooperative step could be to design and construct more transparent non-CPU equipment).
- Procedural issues: a gamma-ray shutter is used, and access control procedures are employed.
- Electronic emanation considerations: a documented commercial RF enclosure is used, together with shielded signal cables and filtered power lines.

Demonstration System IB Summary, continued

- **Multiple intermediate barriers are used to help prevent single-point security failures.**
- **Software, firmware, and CPU operating systems: overly complex software is avoided, and documented source code is provided to the degree possible.**
- **Inputs and outputs: extraneous I/O are removed.**
- **Measurement system authentication and repair: system is designed and constructed to maximize a monitor's ability to examine it before its use or after a repair (plausible procedures are discussed and demonstrated).**

Authentication of Measurement Systems

Purpose of Authentication

- To ensure the monitors that the “host-supplied” equipment is making credible measurements.

Methods of Authentication

- Random selection of equipment
- Use of trusted, unclassified calibration sources
- Thorough system examination by both parties using detailed design documentation

Random Selection of the Equipment

Technique:

- The host supplies multiple identical copies of the measurement equipment.
- The monitor randomly selects
  - one set of equipment for use by both parties during a measurement,
  - one set of equipment for private examination by the monitor.

Feasibility:

- Not really feasible for expensive equipment.
- Not feasible for large fixed installations (will not be employed for the U.S./Russian demo).
- Possible selection of modular subcomponents.
- A potentially fruitful discussion area for subsequent cooperative development.

Trusted Unclassified Calibration Sources

- Issues:
  - Monitor must know and trust the unclassified calibration source characteristics.
    - Monitor may initially provide the sources.
    - Monitor may certify with monitor-supplied equipment.
    - Good source documentation is important.
    - Host will likely retain the calibration sources.
      - Avoids transportation issues.
      - Requires monitor to certify the sources each time.
    - Monitor may even tag plutonium calibration source with a mix of trace radionuclides for later re-certification.
- Another fruitful area for cooperative discussions.
- The U.S. will provide calibration sources for the Russian/U.S. demo and demonstrate plausible certification steps.

Thorough Cooperative Examination Using Complete Documentation Set

- Requires completely inspectable system accompanied by comprehensive documentation set of all hardware and software.
- Monitor allowed private copies of documentation set and of all software sources.
- Host technician measures system parameters for comparison to documentation under monitor direction and supervision during a period of cooperative equipment examination.
- Monitor provided a “certified true” copy of the CPU software for private examination.
  - Host supplies multiple software copies.
  - Monitor selects copy to be used and retains another.
  - Monitor compares and certifies duplicates:
    - byte-for-byte comparison with monitor-supplied/retained computer; and
    - hash function comparison of host CPU memory with monitor’s copy.